

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:)
Isao YAGASAKI, et al.)
Serial No.: To be assigned) Group Art Unit: Unassigned
Filed: December 28, 2000) Examiner: Unassigned



For: **CERTIFICATING SYSTEM FOR PLURALITY OF SERVICES AND METHOD
THEREOF**

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

*Assistant Commissioner for Patents
Washington, D.C. 20231*

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-121581
Filed: April 21, 2000.

It is respectfully requested that the applicants be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

By:

James D. Halsey, Jr.
Registration No. 22,729

Date: December 28, 2000
700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

JC675 U.S. PTO
09/749428
12/28/00

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: April 21, 2000

Application Number: Patent Application
No. 2000-121581

Applicant(s): FUJITSU LIMITED

September 29, 2000

Commissioner,
Patent Office Kozo OIKAWA

Certificate No. 2000-3079682

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application: 2000年 4月21日

出願番号
Application Number: 特願2000-121581

出願人
Applicant(s): 富士通株式会社

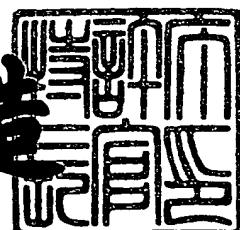


CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 9月29日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3079682

【書類名】 特許願
【整理番号】 0050269
【提出日】 平成12年 4月21日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 15/00
H04L 9/32
【発明の名称】 複数のサービスのための認証システムおよび方法
【請求項の数】 7
【発明者】
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内
【氏名】 矢ヶ崎 功
【発明者】
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内
【氏名】 黒田 俊光
【特許出願人】
【識別番号】 000005223
【氏名又は名称】 富士通株式会社
【代理人】
【識別番号】 100074099
【住所又は居所】 東京都千代田区二番町8番地20 二番町ビル3F
【弁理士】
【氏名又は名称】 大菅 義之
【電話番号】 03-3238-0031
【選任した代理人】
【識別番号】 100067987
【住所又は居所】 神奈川県横浜市鶴見区北寺尾7-25-28-503
【弁理士】

【氏名又は名称】 久木元 彰

【電話番号】 045-573-3683

【手数料の表示】

【予納台帳番号】 012542

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705047

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 複数のサービスのための認証システムおよび方法

【特許請求の範囲】

【請求項1】 複数のサービスに共通の証明書情報を登録する登録手段と、
ユーザが前記複数のサービスのうちの1つのサービスにアクセスするとき、該
ユーザの証明書情報を受け取る受信手段と、

前記ユーザの証明書情報が前記共通の証明書情報に対応するか否かを判定する
判定手段と、

前記ユーザの証明書情報が前記共通の証明書情報に対応するとき、前記1つの
サービスの利用を許可する許可手段と

を備えることを特徴とする認証システム。

【請求項2】 前記1つのサービスのための識別情報とパスワード情報を格
納する格納手段と、該識別情報とパスワード情報に基づいて前記ユーザを認証す
る認証手段と、該ユーザが認証されたとき、前記共通の証明書情報を該ユーザに
発行する発行手段とをさらに備えることを特徴とする請求項1記載の認証シス
テム。

【請求項3】 前記1つのサービスのための識別情報とパスワード情報を格
納する格納手段と、該識別情報とパスワード情報に基づいて前記ユーザを認証す
る認証手段と、該ユーザが認証されたとき、前記共通の証明書情報を失効させる
失効手段とをさらに備えることを特徴とする請求項1記載の認証システム。

【請求項4】 前記複数のサービスを、前記共通の証明書情報により利用可
能なサービスとして登録する利用サービス管理手段をさらに備えることを特徴と
する請求項1記載の認証システム。

【請求項5】 ユーザが1つのサービスにアクセスするとき、該1つのサー
ビスを含む複数のサービスに共通の証明書情報を送出する送信手段と、
前記共通の証明書情報に基づいて前記ユーザが認証されたとき、前記1つのサ
ービスの提供を受けるサービス利用手段と
を備えることを特徴とする端末装置。

【請求項6】 コンピュータのためのプログラムを記録した記録媒体であっ

て、

前記プログラムは、

ユーザが1つのサービスにアクセスするとき、該ユーザの証明書情報を受け取り、

前記ユーザの証明書情報が、あらかじめ登録された、前記1つのサービスを含む複数のサービスに共通の証明書情報に対応するか否かを判定し、

前記ユーザの証明書情報が前記共通の証明書情報に対応するとき、前記1つのサービスの利用を許可する

処理を前記コンピュータに実行させることを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項7】 複数のサービスに共通の証明書情報をあらかじめ登録し、

ユーザが前記複数のサービスのうちの1つのサービスにアクセスするとき、該ユーザの証明書情報が前記共通の証明書情報に対応するか否かを判定し、

前記ユーザの証明書情報が前記共通の証明書情報に対応するとき、該ユーザに対して前記1つのサービスの利用を許可する

ことを特徴とする認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、インターネット等のネットワークを介したサービスに係り、ユーザが複数のサービスを利用する際に、ユーザ認証を行う認証システムおよびその方法に関する。

【0002】

【従来の技術】

ネットワーク上のサービスを提供する提供者は、サービス料金の課金等のために、アクセスしてきたユーザの認証を行う必要がある。従来のサービスシステムでは、1人のユーザが複数のサービスを利用する場合、各サービスが指定する認証方法をユーザ自らが使い分けていた。

【0003】

図14は、このような従来のサービスシステムを示している。2つのサービスA、Bを利用するとき、ユーザ11は、まず、サービスA用の識別情報（ID）とパスワード（PWD）をサービスAのサーバ12に送る。サーバ12は、ユーザ管理データベース（ユーザ管理DB）13を参照してユーザ認証を行った後、ユーザ11にサービスAを提供する。

【0004】

次に、ユーザ11は、サービスB用のIDおよびパスワードをサービスBのサーバ14に送る。サーバ14は、ユーザ管理DB15を参照してユーザ認証を行った後、ユーザ11にサービスBを提供する。こうして、ユーザ11は、ネットワークサービスA、Bを利用することができます。

【0005】

【発明が解決しようとする課題】

しかしながら、上述した従来のサービスシステムには、次のような問題がある

【0006】

1人のユーザが複数のネットワークサービスを利用する場合、各サービスが発行するIDおよびパスワードを使い分ける必要があり、非常に不便である。特に、サービス毎に異なるIDおよびパスワードを用いる場合、ユーザは複数のIDおよびパスワードを記憶しておき、サービス利用時に端末から入力しなければならない。したがって、利用サービスの数が多くなると、ユーザの負担が増大する

【0007】

また、従来のIDおよびパスワードによる認証方法に基づいて、1つのサービスがユーザのIDおよびパスワードを登録し、ユーザがそれらを用いて他のサービスを利用することも考えられる。しかし、各サービスの事業体が異なれば、異なる事業体間で互いにパスワードを教え合うことになり、このような認証方法は、セキュリティの観点から、事実上、実現が困難である。

【0008】

本発明の課題は、複数のサービスのための認証処理において、各サービスが発

行しているパスワード等を互いに知らせることなく、ユーザの負担を軽減する認証システムおよびその方法を提供することである。

【0009】

【課題を解決するための手段】

図1は、本発明の認証システムの原理図である。図1の認証システムは、登録手段21、受信手段22、判定手段23、および許可手段24を備える。

【0010】

登録手段21は、複数のサービスに共通の証明書情報を登録する。受信手段22は、ユーザがそれらの複数のサービスのうちの1つのサービスにアクセスするとき、そのユーザの証明書情報を受け取る。判定手段23は、受け取ったユーザの証明書情報が、登録された共通の証明書情報に対応するか否かを判定する。許可手段24は、ユーザの証明書情報が共通の証明書情報に対応するとき、アクセスされたサービスの利用を許可する。

【0011】

ユーザは、あらかじめ発行された、複数のサービスに共通の証明書情報を保持しており、それらのサービスのうちの1つを利用するとき、ユーザ端末から証明書情報を送出する。

【0012】

受信手段22は、送られた証明書情報を受け取ると、その情報を判定手段23に渡し、判定手段23は、受け取った証明書情報を、登録手段21に登録された証明書情報と比較して、両者が互いに対応するか否かを判定する。判定結果は許可手段24に渡され、許可手段24は、判定結果が2つの証明書情報が互いに対応することを示していれば、ユーザに対してサービスの利用を許可する。

【0013】

このような認証システムによれば、ユーザは、各サービス固有のIDおよびパスワードの代わりに、単一の証明書情報を用いて、複数のサービスを利用することができる。したがって、複数のIDおよびパスワードを扱う必要がなくなり、ユーザの負担が軽減される。

【0014】

例えば、図1の登録手段21は、後述する図2のユーザ情報管理テーブル36、37に対応し、図1の受信手段22、判定手段23、および許可手段24は、図2のサーバ32、33に対応する。あるいはまた、図1の登録手段21は、図2の証明書管理DB35に対応し、図1の受信手段22、判定手段23、および許可手段24は、図2の認証局34に対応する。

【0015】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。

本実施形態の認証システムでは、独立した複数のネットワークサービスに対して、ユーザが1つのデジタル証明書を提示することで、それらのサービスの利用が許可される。このデジタル証明書は、所定の認証方法により認証されたユーザのみに対して発行され、そのユーザが複数のサービスを利用可能であることを表す。

【0016】

デジタル証明書は、ITU-T (International Telecommunication Union Telecommunication Standardization Sector) の仕様X.509に基づき、ユーザ名、証明書発行者名、シリアル番号、ユーザの公開鍵等の情報を統合したデータに、認証局 (Certificate Authority) のデジタル署名を施すことで生成される。この証明書は、中に収められている公開鍵がそこに記されたユーザのものであることを証明している。

【0017】

図2は、このような認証システムにおけるデジタル証明書の発行と審査を示している。図2において、サービスA、Bは、IDおよびパスワードを用いる会員制サービスに対応し、それぞれ、サーバ32、33からユーザ31に対して提供される。認証局34は、これらのサービスの事業体とは独立した証明書発行機関であり、ユーザ31に対して、サービスA、Bに共通のデジタル証明書（共通証明書）を発行する。

【0018】

共通証明書を用いた認証を可能にするためには、あらかじめ、認証局34がユ

ーザ3 1に対してその共通証明書を発行する必要がある。ここでは、認証局3 4は、サービスAを介して共通証明書を発行し、サービスBに対する最初のアクセス時に、サーバ3 3がその共通証明書を審査する。サーバ3 2、3 3は、それぞれ、ユーザ情報管理テーブル3 6、3 7を保持しており、これらのテーブルには、あらかじめ、ユーザ3 1のID、パスワード等が登録されている。この場合、以下のシーケンスに従って処理が行われる。

【0019】

P1：ユーザ3 1は、サービスA用のIDおよびパスワードをサーバ3 2に送る。サーバ3 2は、ユーザ情報管理テーブル3 6を参照してユーザ認証を行い、認証結果がOKであれば、認証局3 4に共通証明書の発行を依頼する。

【0020】

P2：サーバ3 2は、認証局3 4から共通証明書を受け取り、それをユーザ3 1に対して発行する。この段階では、ユーザ3 1が保持する共通証明書は、サービスAを利用する資格のみを有し、認証局3 4の証明書管理DB3 5には、共通証明書の識別情報（例えば、シリアル番号）とともに、対応するユーザ名と、サービスAが利用可能であることを示す情報が登録される。また、ユーザ情報管理テーブル3 6には、IDおよびパスワードとともに、その共通証明書のシリアル番号（Ser. No.）が登録される。

【0021】

P3：ユーザ3 1は、発行された共通証明書をサーバ3 3に提示する。

P4：サーバ3 3は、提示された共通証明書ではサービスBが利用できないと判断し、ユーザ3 1にサービスB用のIDおよびパスワードを要求する。

【0022】

P5：ユーザ3 1は、サービスB用のIDおよびパスワードをサーバ3 3に送る。

P6：サーバ3 3は、ユーザ情報管理テーブル3 7を参照してユーザ認証を行い、認証結果がOKであれば、サービスBをユーザ3 1に提供する。これ以降、ユーザが保持する共通証明書でも、サービスBの利用が可能となる。この段階では、ユーザが保持する共通証明書は、サービスAとサービスBを利用する資格を

有し、証明書管理DB35には、サービスA、Bが利用可能であることを示す情報が登録される。また、ユーザ情報管理テーブル37には、IDおよびパスワードとともに、共通証明書のシリアル番号が登録される。

【0023】

ここでは、P1およびP5の処理において、IDおよびパスワードによるユーザ認証を行っているが、指紋情報、声紋情報、画像情報等による他の認証方法を用いてもよい。また、ユーザは、サービスの利用中止を希望する場合、共通証明書の失効またはサービスの利用禁止の手続きを行う。共通証明書の失効手続きを行う場合、図3に示すように、以下のシーケンスに従って処理が行われる。

【0024】

P11：ユーザ31は、サービスA用のIDおよびパスワード、あるいは共通証明書を、サーバ32に送る。

P12：IDおよびパスワードを受け取った場合、サーバ32は、ユーザ情報管理テーブル36を参照してユーザ認証を行い、認証結果がOKであれば、その旨をユーザ31に通知する。また、共通証明書を受け取った場合、サーバ32は、後述する認証方法でユーザ認証を行い、認証結果をユーザ31に通知する。

【0025】

P13：ユーザ31は、サーバ32に対して、保持している共通証明書の失効依頼を行う。サーバ32は、認証局34に共通証明書のシリアル番号を通知し、失効処理を依頼する。認証局34は、証明書管理DB35からその共通証明書の情報を削除し、サーバ32は、ユーザ情報管理テーブル36からその共通証明書のシリアル番号を削除する。

【0026】

P14：その後、ユーザ31は、保持している共通証明書を、認証情報としてサーバ33に提示する。サーバ33は、提示された共通証明書のシリアル番号を認証局34に通知し、その共通証明書の正当性を問い合わせる。

【0027】

P15：認証局34は、通知されたシリアル番号が証明書管理DB35に登録されていないため、チェック結果がNGであることをサーバ33に通知する。サ

ーバ3 3は、ユーザ情報管理テーブル3 7からその共通証明書のシリアル番号を削除し、サービスBが利用不可であることをユーザ3 1に通知する。

【0028】

図4は、発行された共通証明書を用いたユーザ認証を示している。この場合、以下のシーケンスに従ってサービスが提供される。

P21：ユーザ3 1は、保持している共通証明書を、認証情報としてサーバ3 2に提示する。サーバ3 2は、提示された共通証明書のシリアル番号を認証局3 4に通知し、その共通証明書のチェックを依頼する。認証局3 4は、証明書管理DB3 5を参照して、通知されたシリアル番号が登録されているか否かをチェックする。そして、そのシリアル番号が登録されており、かつ、サービスAが利用可能であれば、チェック結果としてOKを返す。

【0029】

P22：サーバ3 2は、認証局3 4からOKが返されると、サービスAをユーザ3 1に提供する。

P23：ユーザ3 1は、保持している共通証明書を、認証情報としてサーバ3 3に提示する。サーバ3 3は、サーバ3 2と同様にして、認証局3 4からチェック結果を受け取る。

【0030】

P24：サーバ3 3は、認証局3 4からOKが返されると、サービスBをユーザ3 1に提供する。

ここでは、ユーザが2つのサービスを利用する場合について説明したが、3つ以上のサービスを利用する場合も同様である。また、サーバ3 2、3 3は、提示された共通証明書が失効しているか否かを確認するために、認証局3 4に対して共通証明書のチェックを依頼しているが、このチェックを省略することも可能である。

【0031】

この場合、失効処理において、認証局3 4は、失効した共通証明書のシリアル番号を、関連するすべてのサービスのサーバに通知し、各サーバは、ユーザ情報管理テーブルからそのシリアル番号を削除する。そして、ユーザから共通証明書

が提示されたとき、そのシリアル番号が対応するユーザ情報管理テーブルに登録されていれば、認証結果をOKとし、それが登録されていなければ、認証結果をNGとする。

【0032】

図2、3、および4に示した認証システムによれば、ユーザは、各サービス固有のIDおよびパスワードを使用することなく、単一の証明書を提示するだけで、複数のサービスを利用することができます。したがって、複数のIDおよびパスワードを暗記したり、サービス利用時に毎回IDおよびパスワードを入力したりする必要がなくなり、ユーザの負担が大きく軽減される。

【0033】

ところで、証明書管理DB35には、例えば、図5のような証明書管理テーブルと、図6のような利用サービス管理テーブルが格納される。図5の証明書管理テーブルには、共通証明書のシリアル番号、ユーザの氏名、住所、およびeメールアドレスが登録されており、図6の利用サービス管理テーブルには、共通証明書のシリアル番号および利用可能サービスIDが登録されている。証明書管理テーブルおよび利用サービス管理テーブルは、共通証明書毎に生成される。

【0034】

また、図7は、ユーザ情報管理テーブル36、37の例を示している。図7のユーザ情報管理テーブルには、ユーザID、パスワード、ユーザの氏名、住所、および共通証明書のシリアル番号が登録されている。ユーザ情報管理テーブルは、ユーザ毎に生成される。

【0035】

図8は、ユーザ31がサービスAのサーバ32に対して、共通証明書の発行または失効を依頼する場合の処理のフローチャートである。まず、ユーザ31は、サーバ32にアクセスし（ステップS1）、サーバ32は、ユーザ端末にログイン画面を表示する（ステップS2）。次に、ユーザ31は、サービスA用のIDおよびパスワードを入力し（ステップS3）、サーバ32は、ユーザ情報管理テーブル36を参照して、入力されたIDおよびパスワードをチェックする（ステップS4）。

【0036】

IDおよびパスワードが正しくなければ、サーバ32は、ステップS2以降の処理を繰り返す。IDおよびパスワードが正しければ、次に、ユーザ情報管理テーブル36を参照して、対応するユーザに対して共通証明書が発行されているか否かをチェックする（ステップS5）。

【0037】

ユーザ情報管理テーブル36に、そのユーザの共通証明書のシリアル番号が登録されていなければ、共通証明書が発行されていないと判断し、認証局34に共通証明書の発行を依頼する（ステップS6）。

【0038】

これを受け、認証局34は、共通証明書を発行する（ステップS7）。このとき、認証局34は、共通証明書のシリアル番号とユーザ情報を記録した証明書管理テーブルを生成し、共通証明書のシリアル番号とサービスAのIDを記録した利用サービス管理テーブルを生成する。そして、それらのテーブルを証明書管理DB35に格納する。

【0039】

次に、サーバ32は、発行された共通証明書をユーザ31に配布し、ユーザ情報管理テーブル36に、共通証明書のシリアル番号を記録して（ステップS8）、処理を終了する。

【0040】

ステップS5において、ユーザ情報管理テーブル36に共通証明書のシリアル番号が登録されていれば、共通証明書が発行済みであることをユーザ31に通知し、失効を希望するか否かを問い合わせる（ステップS9）。ユーザ31が失効を希望しなければ、そのまま処理を終了する。

【0041】

ユーザ31が失効を希望すれば、登録されている共通証明書のシリアル番号を認証局34に通知し、失効処理を依頼する（ステップS10）。これを受けて、認証局34は、通知されたシリアル番号に対応する証明書管理テーブルおよび利用サービス管理テーブルを削除し、処理結果をサーバ32に通知する。そして、

サーバ32は、ユーザ情報管理テーブル36からその共通証明書のシリアル番号を削除し、共通証明書が失効したことをユーザ31に通知して、処理を終了する。

【0042】

次に、図9は、ユーザ31がサービスBのサーバ33に対して、保持している共通証明書の審査を依頼する場合の処理のフローチャートである。まず、ユーザ31は、サーバ33にアクセスし（ステップS11）、共通証明書を提示する（ステップS12）。

【0043】

次に、サーバ33は、提示された共通証明書のシリアル番号がユーザ情報管理テーブル37に登録されているか否かをチェックする（ステップS13）。そして、そのシリアル番号が登録されていなければ、ステップS14～S16において、図8のステップS2～S4と同様の処理を行う。

【0044】

ステップS16において、IDおよびパスワードが正しければ、次に、サーバ33は、提示された共通証明書のシリアル番号を認証局34に通知し、その共通証明書によるサービスBの利用許可を要請する（ステップS17）。

【0045】

これを受け、認証局34は、通知されたシリアル番号に対応する利用サービス管理テーブルにサービスBのIDを追加し、サービスBが利用可能になったことをサーバ33に通知する（ステップS18）。そして、サーバ33は、ユーザ情報管理テーブル37に、共通証明書のシリアル番号を記録して（ステップS19）、処理を終了する。

【0046】

ステップS13において、共通証明書のシリアル番号がユーザ情報管理テーブル37に登録されていれば、次に、サービスBの利用を禁止するか否かをユーザ31に問い合わせる（ステップS20-1）。そして、ユーザ31が利用禁止を希望しなければ、そのまま処理を終了する。

【0047】

ユーザ31が利用禁止を希望すれば、次に、提示された共通証明書のシリアル番号をユーザ情報管理テーブル37から削除し（ステップS20-2）、その共通証明書の利用可能サービスからサービスBを抹消するように、認証局34に依頼する（ステップS20-3）。

【0048】

これを受け、認証局34は、対応する利用サービス管理テーブルからサービスBのサービスIDを削除し、サービスBを抹消したことをサーバ33に通知する（ステップS20-4）。そして、サーバ33は、サービスBの利用が禁止されたことをユーザ31に通知して、処理を終了する。

【0049】

以上の説明では、証明書管理テーブルと利用サービス管理テーブルを別々に設けているが、これらのテーブルの情報を1つのテーブルにまとめて格納してもよい。

【0050】

次に、図10および図11を参照しながら、インターネット上の会員制サービスであるniftyにおいて、本発明の認証システムを適用した例を説明する。

現在、niftyと連動して各種分野のポータルサイト（portal site）を構築し、多くの企業のサービスを提供する動きが見られる。ポータルサイトは、インターネットの入口となる巨大なWebサイトであり、様々なサービスサイトへのリンクを保持している。しかし、複数の独立したサービスをポータルサイトに集中させると、認証の煩雑さが大きな問題となる。これは、niftyに限らず、どのポータルサイトでも起こり得る問題である。このような場合に、上述した共通認証の仕組みを用いれば、複数のサービスによる認証が簡便化される。

【0051】

図10は、金融関連サービスを提供するポータルサイトFinance@niftyを含むサービスシステムの構成図である。図10のサービスシステムは、インターネット41、認証局のサーバ42、@nifty会員サービスのサーバ43、銀行のサーバ44、クレジット会社のサーバ45、保険会社のサーバ46、インターネットショップのサーバ47、電力会社のサーバ48、ガス会社のサ

ーバ4 9、およびユーザ端末5 0を含む。

【0052】

ここで、@n i f t y、銀行、クレジット会社、保険会社、インターネットショップ、電力会社、およびガス会社は、それぞれ、独立した会員制サービスを提供する事業体に相当する。

【0053】

認証局のサーバ4 2は、証明書管理DB3 5、証明書管理部5 1、およびサービス管理DB5 2を備える。証明書管理DB3 5は、各共通証明書の証明書管理テーブルおよび利用サービス管理テーブルを格納し、証明書管理部5 1は、証明書管理DB3 5を用いて、共通証明書の発行、チェック、失効等の処理を行う。また、サービス管理DB5 2は、各サービスに関する情報を格納し、証明書管理部5 1は、サービス管理DB5 2を用いて、各サービスの入会審査に関する処理を行う。

【0054】

また、@n i f t y会員サービスのサーバ4 3は、会員画面制御部6 1、請求管理部6 2、ユーザ管理DB6 3、画面レイアウトDB6 4、および請求情報DB6 5を備える。ユーザ管理DB6 3は、各ユーザのユーザ情報管理テーブルを格納し、画面レイアウトDB6 4は、会員サービス画面のデータを格納し、請求情報DB6 5は、サーバ4 7、4 8、4 9等から収集される請求金額のデータを格納する。

【0055】

会員画面制御部6 1は、ユーザ管理DB6 3および画面レイアウトDB6 4を用いて、ユーザ端末5 0上の画面表示を制御し、請求管理部6 2は、請求情報DB6 5を用いて、請求金額の表示を制御する。

【0056】

例えば、ユーザ端末5 0の画面に表示されたF i n a n c e @ n i f t yのページ7 1は、会員サービス8 1および証明書8 2の項目を含む。そして、ユーザがこれらの項目を指定すると、ユーザ端末5 0が保持している共通証明書が自動的にサーバ4 3に送られ、認証が行われて、会員メニューのページ7 2が表示さ

れる。このページ72には、公共料金決済サービス83、明細表示サービス84、転居手続きサービス85、および会員設定86の項目が含まれている。

【0057】

このうち、ユーザが公共料金決済サービス83を選択すると、共通証明書がサーバ44に送られ、認証が行われて、公共料金決済のページ73が表示される。このページ73には、口座振替申込み87、インターネット個別払い88、および銀行決済申込み89の項目が含まれている。

【0058】

また、ユーザが明細表示サービス84を選択すると、ユーザの金融情報の明細を示すページ74が表示される。このとき、必要に応じて、共通証明書がサーバ44、45等にも送られ、認証が行われる。

【0059】

このページ74のレイアウトデータは、会員画面制御部61から提供され、請求金額のデータは、請求管理部62から提供される。さらに、銀行口座の残高データは、銀行のサーバ44から提供され、クレジットカードの請求明細のデータは、クレジット会社のサーバ45から提供される。

【0060】

図11は、図10のサービスシステムにおいて、ユーザが明細表示サービス84を利用する場合のシーケンスを示している。この処理においては、以下のシーケンスに従って、@nifaty、銀行、クレジット会社等の複数の事業体のサービスが複合的に提供される。

【0061】

P31：ユーザは、共通証明書を提示して、ユーザ端末50からFinance@nifatyのサイトにアクセスする。

P32：@nifatyのサーバ43は、提示された共通証明書のシリアル番号を、認証局のサーバ42に通知する。

【0062】

P33：サーバ42は、証明書管理DB35の対応する利用サービス管理テーブルを参照し、その共通証明書で@nifaty会員サービスが利用可能であれば

、チェック結果としてOKを返す。

【0063】

P34：サーバ43は、会員メニュー72を表示する。

P35：ユーザは、会員メニュー72から明細表示サービスを選択する。

P36：サーバ43は、共通証明書のシリアル番号を認証局のサーバ42に通知して、利用可能サービスを問い合わせる。

【0064】

P37：サーバ42は、対応する利用サービス管理テーブルを参照して、通知されたシリアル番号に対応する利用可能サービスIDを取得し、それをサーバ43に返す。

【0065】

P38：サーバ43は、受け取った各サービスIDに対応する表示領域を含む、画面描画用のレイアウトデータをユーザ端末50に送る。このレイアウトデータは、HTML (*hypertext markup language*)、XML (*extensible markup language*) 等で記述される。

【0066】

P39：ユーザ端末50は、共通証明書を提示して、A銀行のサーバに明細情報問い合わせる。

P40：A銀行のサーバは、提示された共通証明書のシリアル番号を、認証局のサーバ42に通知する。

【0067】

P41：サーバ42は、証明書管理DB35の対応する利用サービス管理テーブルを参照し、その共通証明書でA銀行のサービスが利用可能であれば、チェック結果としてOKを返す。

【0068】

P42：A銀行のサーバは、ユーザ口座の残高データを、明細情報としてユーザ端末50に送る。

P43～P46：B銀行のサーバも、A銀行のサーバと同様にして、共通証明書による認証に基づいて、ユーザ口座の残高データをユーザ端末50に送る。

【0069】

こうして、ユーザ端末50の画面に、明細ページ74が表示される。クレジット会社のサーバ45や保険会社のサーバ46も、同様のシーケンスで、明細ページ74に明細情報を提供することができる。

【0070】

図10のサービスシステムによれば、各サービスが別々に保持している口座残高や請求金額等の明細情報を、1つのレイアウト画面上に統合して表示することができ、複数のサービスの横断利用が可能になる。図10においては、認証局の機能が各サービスから独立しているが、この機能を@nifty会員サービスの中に取り込んでもよい。

【0071】

図10のサーバ42～49およびユーザ端末50は、例えば、図12に示すような情報処理装置（コンピュータ）を用いて構成することができる。図12の情報処理装置は、CPU（中央処理装置）91、メモリ92、入力装置93、出力装置94、外部記憶装置95、媒体駆動装置96、およびネットワーク接続装置97を備え、それらはバス98により互いに接続されている。

【0072】

メモリ92は、例えば、ROM (read only memory)、RAM (random access memory) 等を含み、処理に用いられるプログラムとデータを格納する。CPU91は、メモリ92を利用してプログラムを実行することにより、必要な処理を行う。

【0073】

例えば、図10の証明書管理部51、会員画面制御部61、および請求管理部62は、プログラムにより記述されたソフトウェアコンポーネントとしてメモリ92に格納される。

【0074】

入力装置93は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、オペレータ（サービス運用者またはユーザ）からの指示や情報の入力に用いられる。出力装置94は、例えば、ディスプレイ、プリンタ、スピーカ

等であり、オペレータへの問い合わせや処理結果の出力に用いられる。

【0075】

外部記憶装置95は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク(magneto-optical disk)装置、テープ装置等である。情報処理装置は、この外部記憶装置95に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ92にロードして使用する。また、外部記憶装置95は、図10の証明書管理DB35、サービス管理DB52、ユーザ管理DB63、画面レイアウトDB64、および請求情報DB65としても利用される。

【0076】

媒体駆動装置96は、可搬記録媒体99を駆動し、その記録内容にアクセスする。可搬記録媒体99としては、メモリカード、フロッピーディスク、CD-ROM(compact disk read only memory)、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体が用いられる。オペレータは、この可搬記録媒体99に上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ92にロードして使用する。

【0077】

ネットワーク接続装置97は、インターネット41等の任意の通信ネットワークに接続され、通信に伴うデータ変換を行う。また、情報処理装置は、上述のプログラムとデータをネットワーク接続装置97を介して他の装置から受け取り、必要に応じて、それらをメモリ92にロードして使用する。

【0078】

図13は、図12の情報処理装置にプログラムとデータを供給することのできるコンピュータ読み取り可能な記録媒体を示している。可搬記録媒体99や外部のデータベース100に保存されたプログラムとデータは、メモリ92にロードされる。そして、CPU91は、そのデータを用いてそのプログラムを実行し、必要な処理を行う。

【0079】

以上説明した実施形態においては、ITU-Tの仕様X.509に基づくデジタル証明書を認証情報として用いているが、必要に応じて、他の仕様の証明書情

報を用いてもよい。

【0080】

【発明の効果】

本発明によれば、複数のサービスに共通の1つの認証情報により、各サービスによる認証が可能になる。このため、ユーザは、各サービスが発行するIDおよびパスワードを使い分ける必要がなくなり、ユーザの負担が軽減される。また、異なるサービス間でパスワード等を互いに知らせる必要がなく、セキュリティが保持される。

【図面の簡単な説明】

【図1】

本発明の認証システムの原理図である。

【図2】

証明書の発行と審査を示す図である。

【図3】

証明書の失効を示す図である。

【図4】

証明書による認証を示す図である。

【図5】

証明書管理テーブルを示す図である。

【図6】

利用サービス管理テーブルを示す図である。

【図7】

ユーザ情報管理テーブルを示す図である。

【図8】

証明書の発行／失効処理のフローチャートである。

【図9】

証明書の審査処理のフローチャートである。

【図10】

サービスシステムの構成図である。

【図1 1】

複数サービスの利用例を示す図である。

【図1 2】

情報処理装置の構成図である。

【図1 3】

記録媒体を示す図である。

【図1 4】

従来のサービスシステムを示す図である。

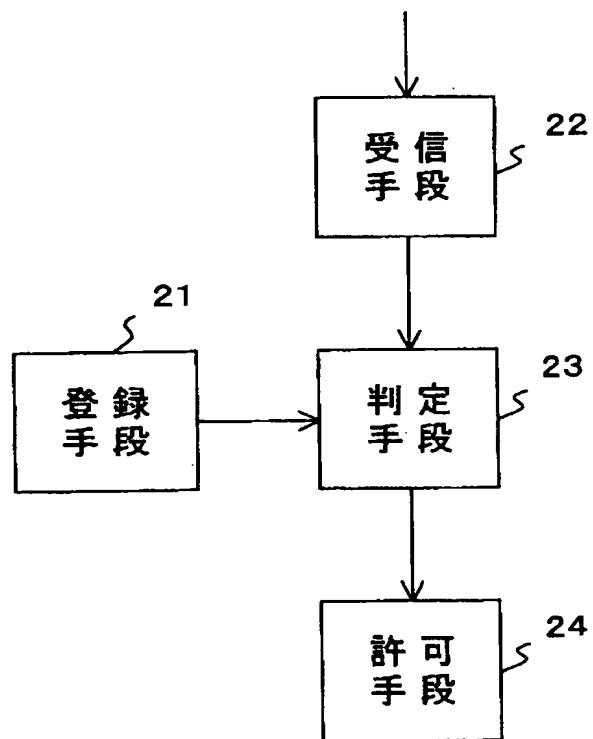
【符号の説明】

- 1 1、 3 1 ユーザ
- 1 2、 3 2 サービスAのサーバ
- 1 3、 1 5 ユーザ管理DB
- 1 4、 3 3 サービスBのサーバ
- 2 1 登録手段
- 2 2 受信手段
- 2 3 判定手段
- 2 4 許可手段
- 3 4 認証局
- 3 5 証明書管理DB
- 3 6、 3 7 ユーザ情報管理テーブル
- 4 1 インターネット
- 4 2 認証局のサーバ
- 4 3 @nift.y会員サービスのサーバ
- 4 4 銀行のサーバ
- 4 5 クレジット会社のサーバ
- 4 6 保険会社のサーバ
- 4 7 インターネットショップのサーバ
- 4 8 電力会社のサーバ
- 4 9 ガス会社のサーバ

- 5 0 ユーザ端末
- 5 1 証明書管理部
- 5 2 サービス管理DB
- 6 1 会員画面制御部
- 6 2 請求管理部
- 6 3 ユーザ管理DB
- 6 4 画面レイアウトDB
- 6 5 請求情報DB
- 7 1 f i n a n c e @ n i f t y のページ
- 7 2 会員メニューのページ
- 7 3 公共料金決済のページ
- 7 4 明細ページ
- 8 3 公共料金決済サービス
- 8 4 明細表示サービス
- 8 5 転居手続きサービス
- 8 6 会員設定
- 8 7 口座振替申込み
- 8 8 インターネット個別払い
- 8 9 銀行決済申込み
- 9 1 C P U
- 9 2 メモリ
- 9 3 入力装置
- 9 4 出力装置
- 9 5 外部記憶装置
- 9 6 媒体駆動装置
- 9 7 ネットワーク接続装置
- 9 8 バス
- 9 9 可搬記録媒体
- 1 0 0 データベース

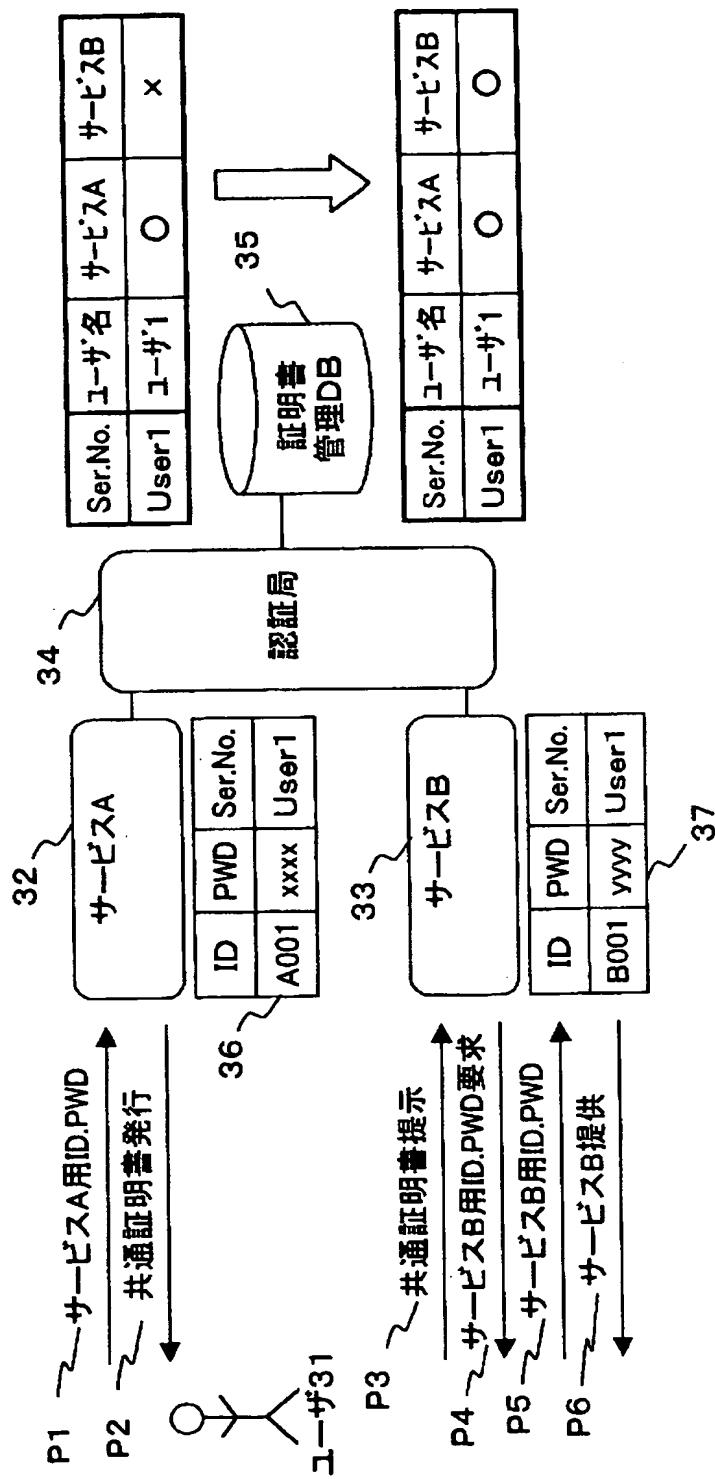
【書類名】 図面
【図1】

本発明の原理図



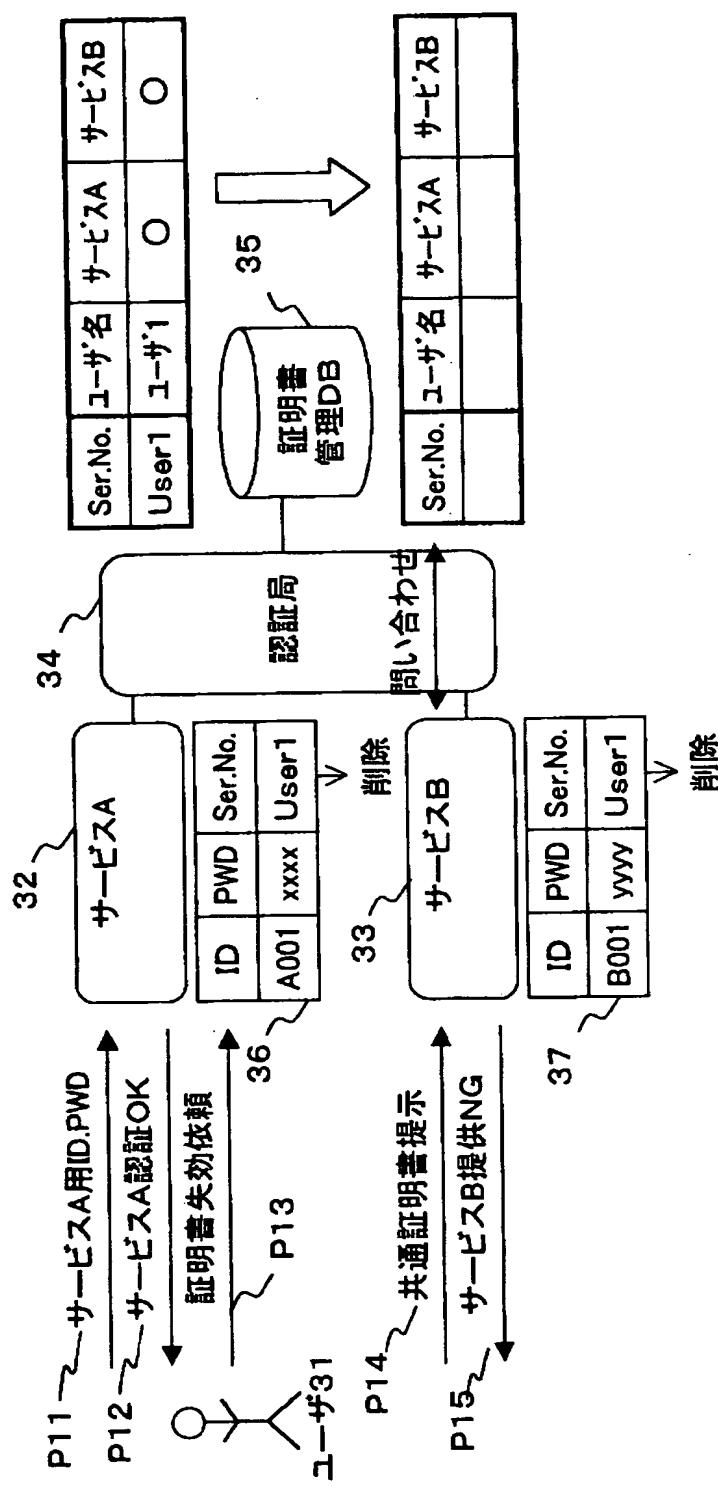
【図2】

証明書の発行と審査を示す図



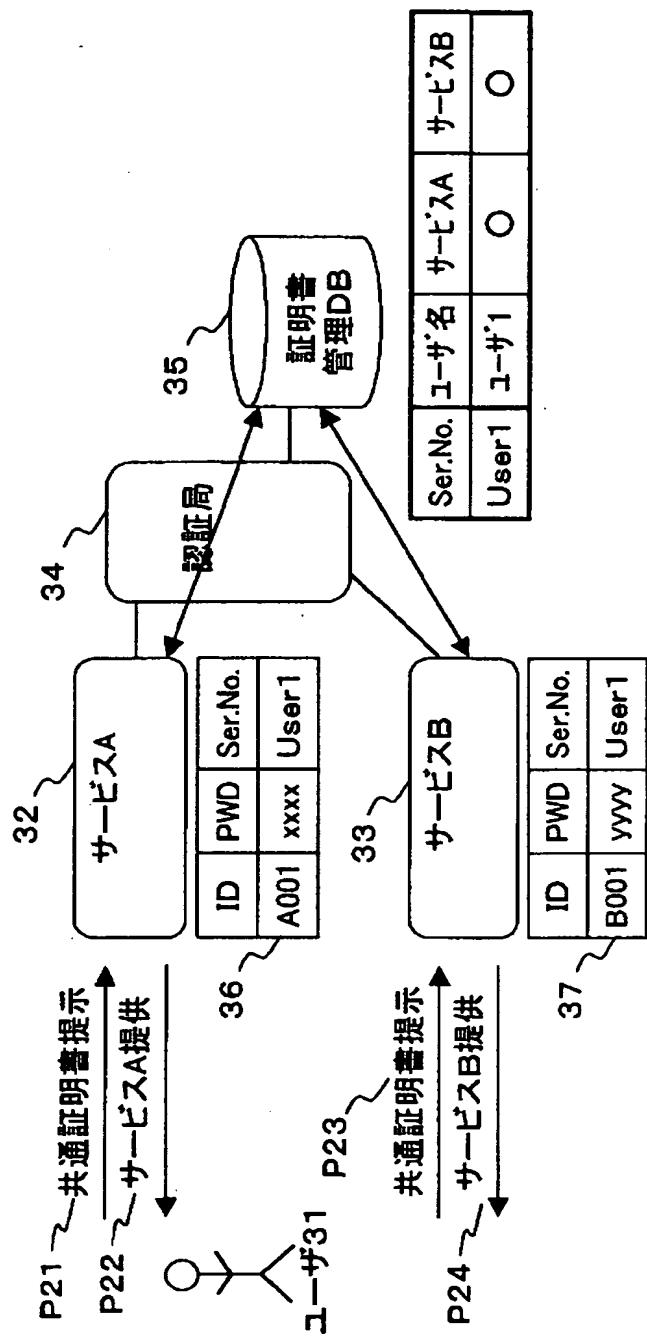
【図3】

証明書の失効を示す図



【図4】

証明書による認証を示す図



【図5】

証明書管理テーブルを示す図

証明書Ser. No.	User0001
氏名	富士通太郎
住所	東京都大田区
eメールアドレス	xxx@xxx.jp

【図6】

利用サービス管理テーブルを示す図

証明書Ser. No.	User0001
利用可能サービスID	Service A Service B

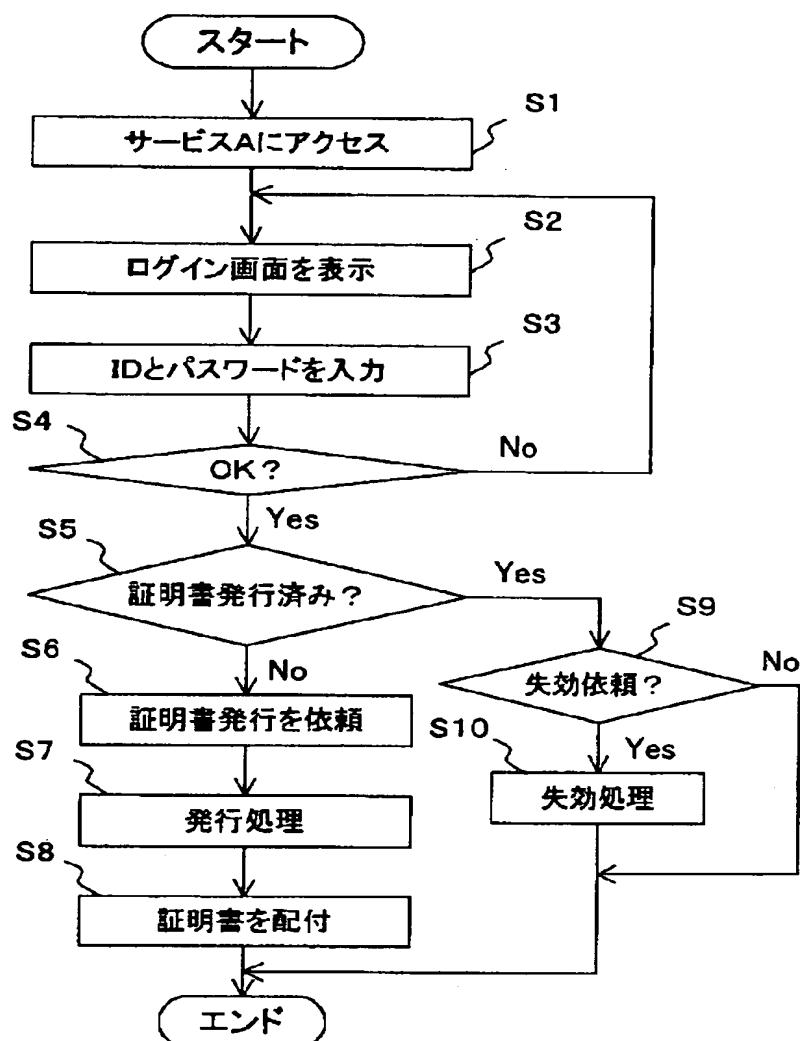
【図7】

ユーザ情報管理テーブルを示す図

ユーザID	AAA00000
パスワード	XXXXXX
氏名	富士通太郎
住所	東京都大田区
証明書Ser. No.	User0001

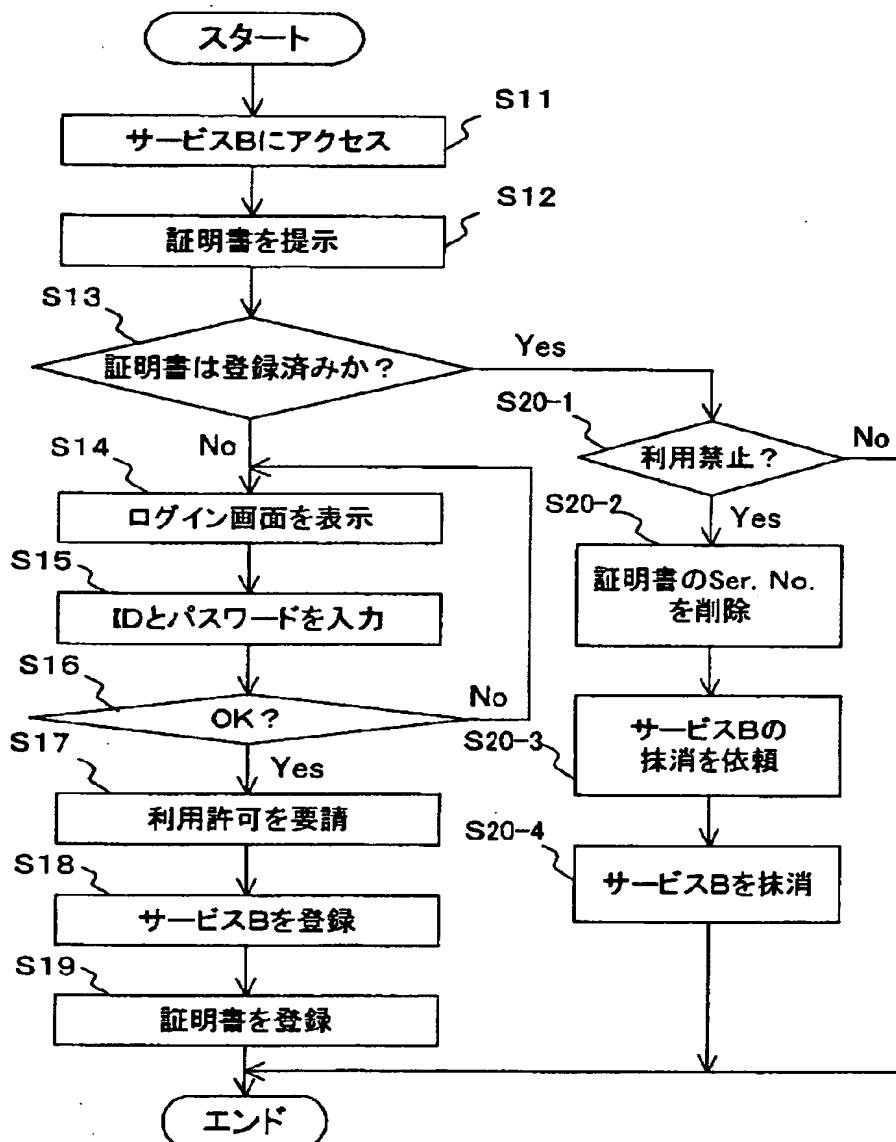
【図8】

証明書の発行／失効処理のフローチャート



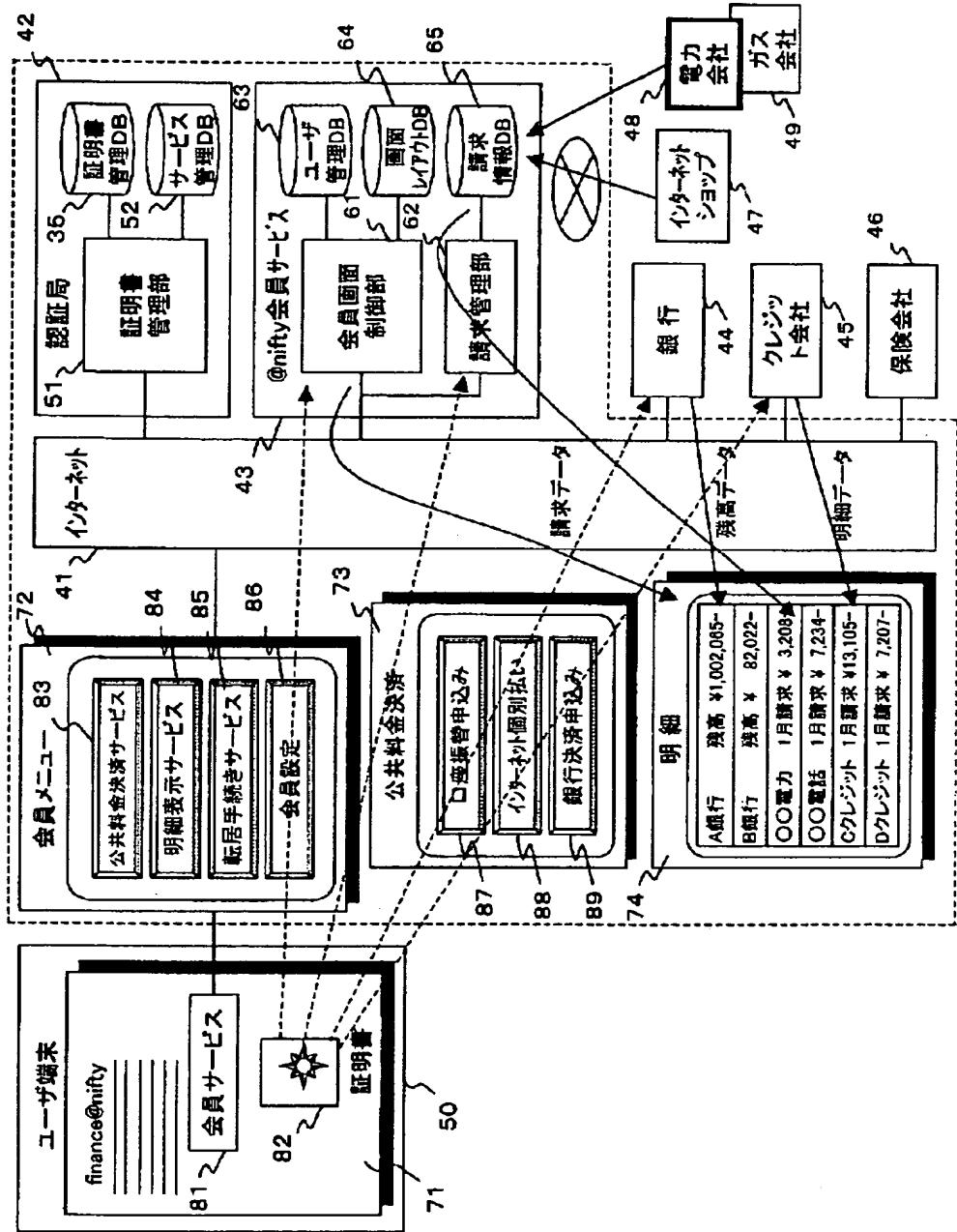
【図9】

証明書の審査処理のフローチャート



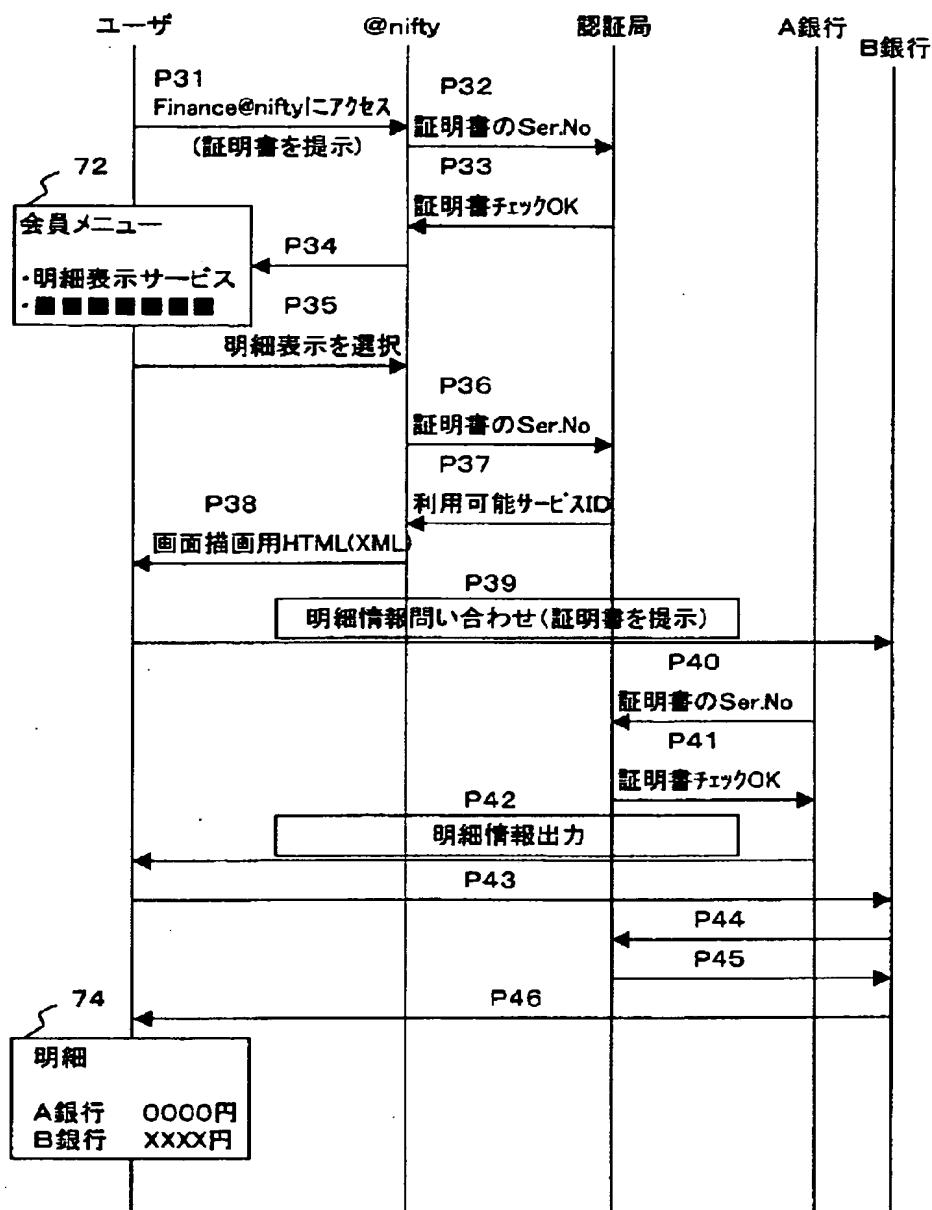
【図10】

サービスシステムの構成図



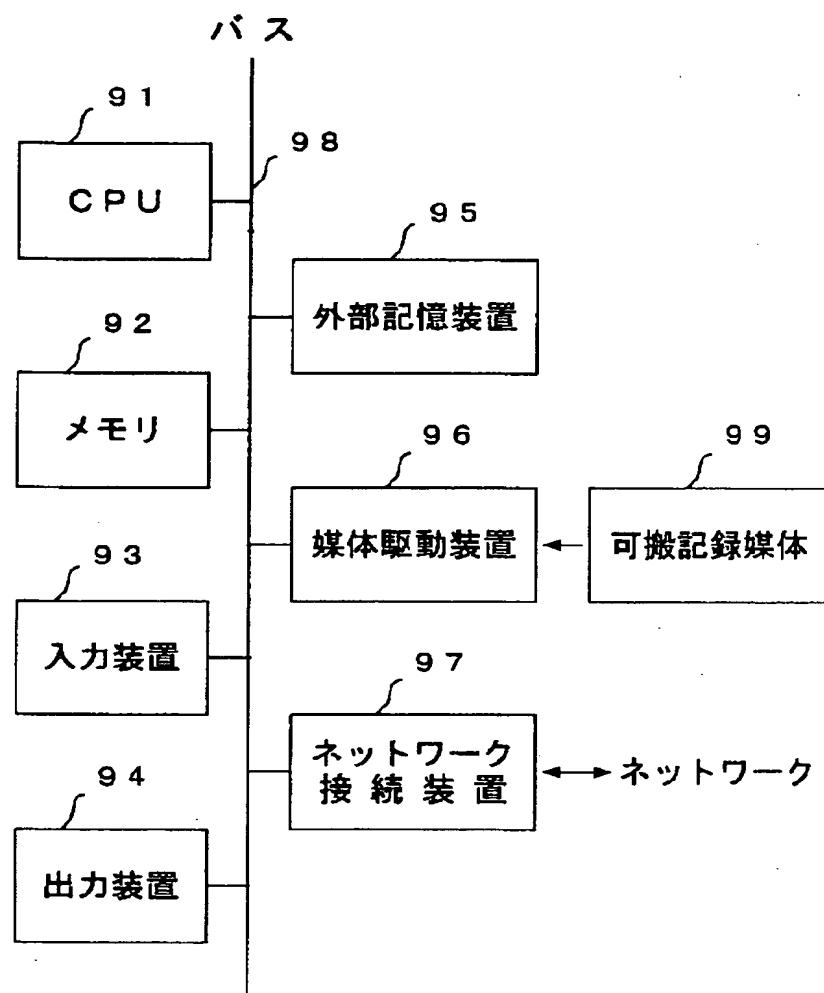
【図11】

複数サービスの利用例を示す図



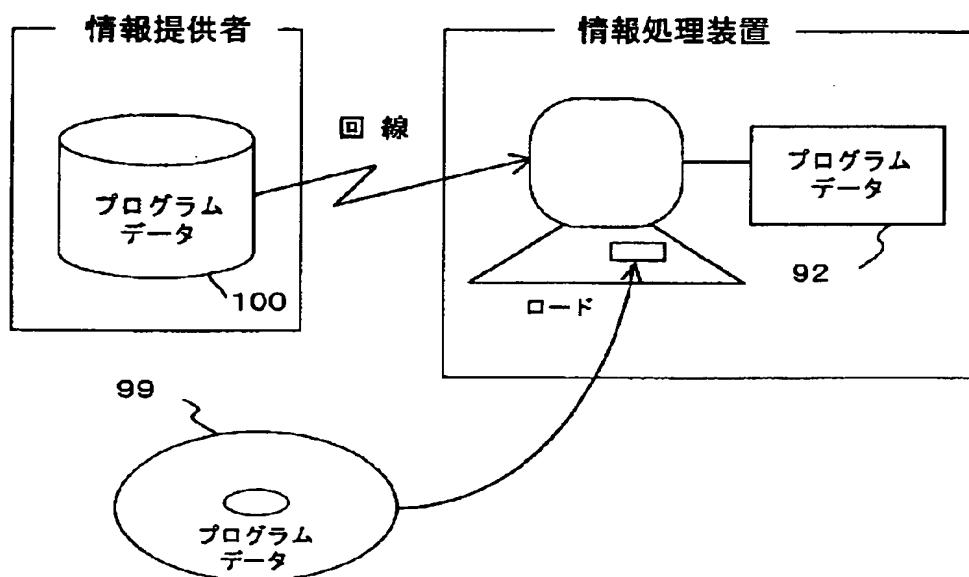
【図12】

情報処理装置の構成図



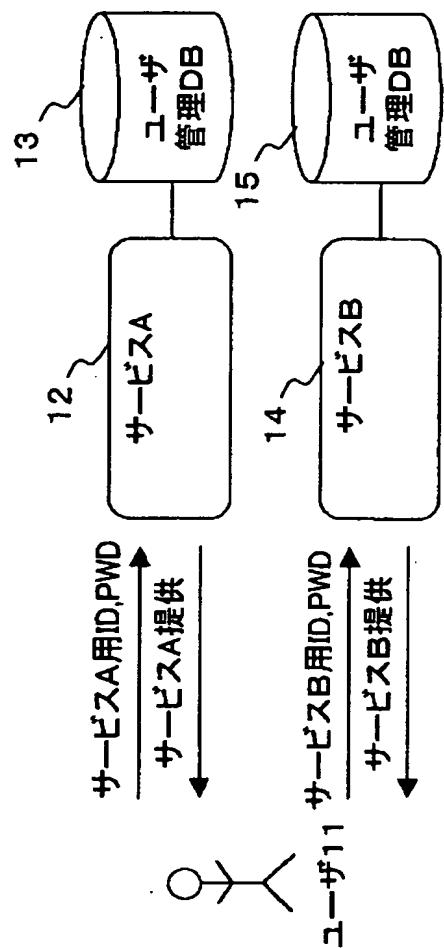
【図13】

記録媒体を示す図



【図14】

従来のサービスシステムを示す図



【書類名】 要約書

【要約】

【課題】 ネットワーク上の複数のサービスのための認証処理において、ユーザの負担を軽減することが課題である。

【解決手段】 ユーザ31は、共通証明書をサービスAのサーバ32に提示し（P21）、サーバ32は、提示された共通証明書のシリアル番号を認証局34に通知する。認証局34は、証明書管理DB35を参照して、通知されたシリアル番号が登録されており、かつ、サービスAが利用可能であれば、OKを返す。これを受け、サーバ32は、サービスAをユーザ31に提供する（P22）。同様にして、ユーザ31が共通証明書をサービスBのサーバ33に提示すると（P23）、サーバ33は、サービスBをユーザ31に提供する（P24）。

【選択図】 図4

出願人履歴情報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社